IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application for:

COMPOSITE SESSION-BASED ENCRYPTION OF VIDEO ON DEMAND CONTENT

Inventor(s): Leo Mark Pedlow, Jr.

Docket Number: SNY-T5775.02

Prepared By:

Miller Patent Services
2500 Dockery Lane
Raleigh, NC 27606

Phone: (919) 816-9981
Fax: (919) 816-9982
Email: miller@patent-inventions.com

CERTIFICATE OF EXPRESS MAILING FOR NEW PATENT APPLICATION

"Express Mail" mailing label number: ER 999163735 US

Date of Deposit: 4-13-04

I Hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.

Typed or printed name of person mailing paper or fee: Catherine N. Miller

Signature of person mailing paper or fee: Catherine N. Miller

COMPOSITE SESSION-BASED ENCRYPTION OF VIDEO ON DEMAND CONTENT

CROSS REFERENCE TO RELATED DOCUMENTS

This application is related to and claims priority benefit of U.S. Provisional Patent Application Serial No. 60/530,071 filed December 16, 2003 to Pedlow for "Composite Session Based Encryption of Video On Demand Content" which is hereby incorporated by reference. This application is also related to U.S. Patent Applications docket number SNY-R4646.01 entitled "Critical Packet Partial Encryption" to Unger et al., serial number 10/038,217; patent applications docket number SNY-R4646.02 entitled "Time Division Partial Encryption" to Candelore et al., serial number 10/038,032; docket number SNY-R4646.03 entitled "Elementary Stream Partial Encryption" to Candelore, serial number 10/037,914; docket number SNY-R4646.04 entitled "Partial Encryption and PID Mapping" to Unger et al., serial number 10/037,499; and docket number SNY-R4646.05 entitled "Decoding and Decrypting of Partially Encrypted Information" to Unger et al., serial number 10/037,498 all of which were filed on January 2, 2002 and are hereby incorporated by reference herein.

COPYRIGHT NOTICE

BACKGROUND

The Passage™ initiative (Passage is a trademark of Sony Electronics Inc.), promoted by Sony, provides a mechanism for MSOs (Multiple Service Operators) to deploy non-legacy headend equipment, subscriber devices and services on their existing legacy networks. In the USA, these networks are most commonly supplied by either Motorola (former General Instrument) or Scientific Atlanta. These two companies at present constitute better than a 99% share of the US cable system market as turnkey system providers. The systems, by design, employ proprietary technology and interfaces precluding the introduction of non-incumbent equipment into the network. An MSO, once choosing one of these suppliers during conversion from an analog cable system to a digital cable system, faces a virtual monopoly when seeking suppliers for additional equipment as their subscriber base or service offering grows.

Before the Passage™ initiative, the only exit from this situation was to forfeit the considerable capital investment already made with the incumbent provider, due to the intentional incompatibility of equipment between the incumbent and other sources. One primary barrier to interoperability is in the area of conditional access systems, the heart of addressable subscriber management and revenue collection resources in a modern digital cable network.

The Passage™ technologies were developed to allow the independent coexistence of two or more conditional access systems on a single, common plant. Unlike other attempts to address the issue, the two systems operate with a common transport stream without any direct or indirect interaction between the conditional access systems. The basic processes used in these technologies are discussed in detail in the above-referenced pending patent applications.

The above-referenced commonly owned patent applications, and others, describe inventions relating to various aspects of methods generally referred to herein as partial encryption or selective encryption, consistent with certain aspects of Passage™. More particularly, systems are described therein wherein selected portions of a particular selection of digital content are encrypted using two (or more) encryption techniques

while other portions of the content are left unencrypted. By properly selecting the portions to be encrypted, the content can effectively be encrypted for use under multiple decryption systems without the necessity of encryption of the entire selection of content. In some embodiments, only a few percent of data overhead is consumed to effectively encrypt the content using multiple encryption systems. This results in a cable or satellite system being able to utilize Set-top boxes (STB) or other implementations of conditional access (CA) receivers from multiple manufacturers in a single system - thus freeing the cable or satellite company to competitively shop for providers of Set-top boxes.

In each of these disclosures, the clear content is identified using a primary Packet Identifier (PID). A secondary PID (or shadow PID) is also assigned to the program content. Selected portions of the content are encrypted under two (or more) encryption systems and the encrypted content transmitted using both the primary and secondary PIDs (one PID or set of PIDs for each encryption system). The so-called legacy STBs operate in a normal manner decrypting encrypted packets arriving under the primary PID and ignoring secondary PIDs. The newer (non-legacy) STBs operate by associating both the primary and secondary PIDs with a single program. Packets with a primary PID are decoded normally and packets with a secondary PID are first decrypted then decoded. The packets associated with both PIDs are then assembled together to make up a single program stream. The PID values associated with the packets are generally remapped to a single PID value for decoding (shadow PIDs remapped to the primary PID value or vice versa.)

BRIEF DESCRIPTION OF THE DRAWINGS

Certain illustrative embodiments illustrating organization and method of operation, together with objects and advantages may be best understood by reference detailed description that follows taken in conjunction with the accompanying drawings in which:

FIGURE 1 is a block diagram of a clear video VOD system.

FIGURE 2 is a block diagram of a composite session based encrypted VOD architecture consistent with certain embodiments of the present invention.

FIGURE 3 is a flow chart depicting operation of a composite session based encrypted VOD embodiment consistent with certain embodiments of the present invention.

ACRONYMS, ABBREVIATIONS AND DEFINITIONS

ASI - Asynchronous Serial Interface

CA - Conditional Access

CASID - Conditional Access System Identifier

CPE - Customer Premises Equipment

DHEI - Digital Headend Extended Interface

ECM - Entitlement Control Message

EPG - Electronic Program Guide

GOP - Group of Pictures (MPEG)

MPEG - Moving Pictures Experts Group

MSO - Multiple System Operator

OLES – Off Line Encryption System

PAT - Program Allocation Table

PID - Packet Identifier

PMT - Program Map Table

PSI - Program Specific Information

QAM - Quadrature Amplitude Modulation

RAM - Random Access Memory

RAID - Redundant Array of Independent Disks

SAN - Storage Area Network

VOD - Video on Demand

Critical Packet - A packet or group of packets that, when encrypted, renders a portion of a video image difficult or impossible to view if not properly decrypted, or which renders

a portion of audio difficult or impossible to hear if not properly decrypted. The term "critical" should not be interpreted as an absolute term, in that it may be possible to hack an elementary stream to overcome encryption of a "critical packet", but when subjected to normal decoding, the inability to fully or properly decode such a "critical packet" would inhibit normal viewing or listening of the program content.

Selective Encryption (or Partial Encryption) – encryption of only a portion of an elementary stream in order to render the stream difficult or impossible to use (i.e., view or hear).

Dual Selective Encryption – encryption of portions of a single selection of content under two separate encryption systems.

Passage™ - Trademark of Sony Electronics Inc. for various single and multiple selective encryption systems, devices and processes.

Trick mode – an operational mode of playback of digital content to simulate fast forward, rewind, pause, suspend (stop), slow motion, etc. operations as in a video tape system.

The terms "a" or "an", as used herein, are defined as one, or more than one. The term "plurality", as used herein, is defined as two or more than two. The term "another", as used herein, is defined as at least a second or more. The terms "including" and/or "having", as used herein, are defined as comprising (i.e., open language). The term "coupled", as used herein, is defined as connected, although not necessarily directly, and not necessarily mechanically. The term "program", as used herein, is defined as a sequence of instructions designed for execution on a computer system. A "program", or "computer program", may include a subroutine, a function, a procedure, an object method, an object implementation, in an executable application, an applet, a servlet, a source code, an object code, a shared library / dynamic load library and/or other sequence of instructions designed for execution on a computer system.

The terms "scramble" and "encrypt" and variations thereof may be used synonymously herein. Also, the term "television program" and similar terms can be interpreted in the normal conversational sense, as well as a meaning wherein the term

means any segment of A/V content that can be displayed on a television set or similar monitor device. The term "video" is often used herein to embrace not only true visual information, but also in the conversational sense (e.g., "video tape recorder") to embrace not only video signals but associated audio and data. The term "legacy" as used herein refers to existing technology used for existing cable and satellite systems. The exemplary embodiments of VOD disclosed herein can be decoded by a television Set-Top Box (STB), but it is contemplated that such technology will soon be incorporated within television receivers of all types whether housed in a separate enclosure alone or in conjunction with recording and/or playback equipment or Conditional Access (CA) decryption module or within a television set itself.

DETAILED DESCRIPTION

While this invention is susceptible of embodiment in many different forms, there is shown in the drawings and will herein be described in detail specific embodiments, with the understanding that the present disclosure of such embodiments is to be considered as an example of the principles and not intended to limit the invention to the specific embodiments shown and described. In the description below, like reference numerals are used to describe the same, similar or corresponding parts in the several views of the drawings.

CLEAR VOD ARCHITECTURES

The decision on a particular VOD architecture is the result of the interaction between a complex set of both independent and dependent variables, providing a solution to an equation of state. Some of the variables are fixed directly as a result of choices by the MSO. Others are constrained by factors such as the existing incumbent system, location, size, available capital and return on investment requirements.

A generalized VOD system 10, as shown in **FIGURE 1**, contains some or all of the following elements / resources: Content Aggregation and Asset management 14, Content distribution (SAN) 18, Video server module(s) 22, Session Management 26,

Transaction management 30, Billing system 34, EPG server or VOD catalog server 38, Transport router/switch fabric (routing matrix) 42, Stream encryption device(s) (not shown in this Figure), and QAM modulators/upconverters and other edge resources 46. This VOD system 10 provides programming to the subscriber terminals such as 50 for ultimate viewing and listening on a TV set or other monitor device 54.

In operation, content is received from various sources including, but not limited to, satellite broadcasts received via one or more satellite dishes 58. Content is aggregated at 14 and cataloged at EPG server or VOD catalog server 38. Content is then distributed at 18 to one or more video servers 22. When a subscriber orders a VOD selection, a message is sent from the subscriber terminal (e.g., STB) 50 to the session manager 26. The session manager 26 notifies the transaction manager 30 to assure that the billing system 34 is properly brought into play. The session manager 26 selects a VOD server from a cluster of VOD servers having the requested content on it and having a signal path that reaches the node serving the subscriber. The session manager also enables the routing matrix 42 to properly route the selected video content through the correct edge resources 46 for delivery to the subscriber terminal 50.

VOD PROGRAM SPECIFIC INFORMATION

A function of the VOD video server(s) 22, in addition to origination of session A/V content, is the creation of the associated, session specific PSI (program specific information). This information is a departure from the broadcast model in that the PSI is extremely dynamic. The content of the PAT and subordinate PMTs change whenever a new session is started or ended. In the broadcast world, the PSI changes very seldom because the PSI tables reflect only the structure of the transport multiplex, not the actual A/V content carried within.

The VOD video server 22 or associated headend hardware or software dynamically assigns a new session to an existing, available "slot" in an outgoing transport multiplexed stream. The slot is denoted by the MPEG program number and in many cases, the combination of which transport stream (TSID) and program number determine

at the service level a unique session and the routing that occurs as a result. Edge resources 46 generally are not configured dynamically. The routing of content appearing on a particular input port to a specific QAM carrier at the output is determined through a preconfigured, static assignment of TSID/input port and program number mapping to specific QAM resources in the device. This same mapping information is also loaded in the VOD system so that once a session is requested by and authorized for a specific subscriber terminal 50, a solution to a routing matrix 42 can be determined to find the appropriate VOD server 22 and QAM transport 46 serving the requestor. This solution also considers dynamic issues such as which servers 22 the requested asset is loaded upon, and server loading/available slots in addition to the simpler, static solution to finding the first possible path to the requesting subscriber terminal 50.

In addition to solving the routing matrix 42 and provisioning the session with PIDs and PSI appropriate to follow the intended route, elements of the same information (program ID and QAM frequency) are also communicated to the session client at subscriber terminal 50 at the subscriber's premises so that the requested stream can be properly received and presented to the subscriber.

CLEAR VOD DISTRIBUTION

Perhaps the simplest VOD implementation is a clear VOD distribution system, i.e. one that contains no encryption as depicted in **FIGURE 1**. While not providing any safekeeping of what might be considered the entertainment medium's most valuable properties, namely current feature films, etc., clear VOD avoids many of the issues that the incumbent cable system providers to date have not adequately addressed and that introduction of a second, alternative CA system complicates even further still. Various arrangements for providing selective or full encryption in a VOD environment are discussed below. Throughout this discussion, it is instructive to carry an example VOD movie through the various embodiments to illustrate the relative storage efficiencies obtained with the various systems disclosed. A real world example of a VOD movie which will be used throughout this document has the following attributes:

Compressed video data rate:	3Mbit/S
Movie length:	120 minutes (2 Hrs)
I-frame overhead:	17%
Total storage used for the video portion of a single, clear (unencrypted) copy of a film:	**3.618GBytes.**

SESSION-BASED ENCRYPTION VOD DISTRIBUTION

In session based encryption, a basic premise is that a classic (clear) VOD server 22 such as shown in **FIGURE 1**, is modified to add an encryption device in series with the transport stream between the video server 22 and the QAM modulator of 46. In certain embodiments, the encryption device may be integrated with the QAM modulator 46 and/or other components. The commercially available Scientific-Atlanta MQAM and Harmonic NSG products are commercial examples of such devices.

The outgoing transport stream, containing multiple, independent VOD sessions and serving multiple subscribers, is encrypted at the point of distribution to the plant and in turn to the subscribers. The control of the encryption and entitlements is based upon interaction between the session manager 26, which controls the session, video server 22 and the conditional access system through defined interfaces. Many session based VOD architectures share the following common drawbacks:

- Coordination and/or distribution of entitlements and synchronization between session manager, conditional access system and stream encryption device.
- Security of the clear content from theft or piracy before loading on the video server and while stored in the system.
- Additional costs for adding both legacy and alternate stream encryption devices.
- Availability of legacy stream encryption devices with reasonable densities (session capacity).

- According to MSOs familiar with the subject, session based VOD streams are unsupported by certain existing conditional access technologies.
- With session-based encryption (compared to the pre-encryption scheme) additional security is afforded by the application of unique encryption keys used for every session of the same program.

In most cases, the video server does not need to generate special PSI that is aware of the conditional access method used for a specific session. The encryption device(s) downstream of the video server will append CA information specific to each session processed at the time/point of encryption. The VOD session manager 26 manages which streams are processed by which CA method and in some cases, manages dynamically routing the streams to/through the encryption devices appropriate for a particular session.

As with other architectures, there are variations on the basic architecture of the session-based system and some of those variations are described below.

COMPOSITE SESSION BASED ENCRYPTION

The composite session based encryption approach is a type of session-based approach that allows multiple conditional access systems to operate in a single VOD system. In this arrangement, as depicted in **FIGURE 2**, the appropriately encrypted stream is provided to a subscriber by routing the outgoing stream from the VOD server 22 to the subscriber terminal 50 on a transport stream and resultant RF carrier, carrying multiple conditional access formats and multiple sessions in a single heterogeneously encrypted multiplex. There is no sharing of resources between the CA systems and they operate independently. A single transport may contain any combination of two or more CA formats operating independently on a program basis representing individual subscriber sessions.

In this embodiment, during loading of the new content on the VOD server 22, the content is processed by the VOD server 22 through internal software, or by an external device such as selective encryption processor 104. This process identifies and segregates "critical" packets (see definition above) using any suitable selective encryption selection

process. That is, it identifies packets that are to be encrypted later. The "critical" packets are segregated by associating them with one or more new, previously unused PIDs. The composite stream made up of the original bulk, "non-critical" content and segregated "critical" content can be either stored as a single asset (e.g., a single file) on the VOD server 22 or the content may be stored in two separate files ("critical" and "non-critical") with each transmitted separately. Also alternatively, new PIDs could be assigned to each of the "critical" and "non-critical" content. In either case, the content can be stored unencrypted (in the clear).

If one refers to the example movie scenario described above, the same movie using 3.618GB of storage in the clear VOD state would require 3.618GBytes to store using composite session based encryption supporting two (or more) different CA systems.

When a subscriber terminal 50 requests VOD content from the headend, the session manager 26 provisions either the legacy CA system 108 or the alternate CA system 112 (depending upon whether the subscriber terminal 50 is capable of legacy or alternate decryption). If the subscriber terminal 50 is legacy decryption compatible, the legacy CA system 108 in turn provisions the legacy encryption device(s) to carry out the encryption process. In this example, the legacy encryption device 116 is configured to encrypt packets identified by the new PIDs associated with "critical" content and the content is routed from VOD server 22 by routing matrix 120 the legacy encryption device 116. The "non-critical" content bypasses the legacy encryption device altogether and is routed by routing matrix 120 directly to routing matrix 124 by path 134.

After encryption at 116, the selectively encrypted content along with the non-"critical" content received via route 134 is routed by routing matrix 124 through add/drop re-multiplexer 128, alternate encryption device 132 and edge resources 46 to the subscriber terminal 50. In this embodiment, the alternate encryption device 132 simply passes the content without acting on it since the alternate encryption device 132 has not been configured to carry out encryption of the content passing therethrough. In this example, the add/drop re-multiplexer 128 reconstitutes the content from legacy

encryption device 116 and from path 134 into a single stream by interleaving the incoming packets ("critical" and "non-critical") into a single correctly ordered stream. Add/drop re-multiplexer serves to re-clock the stream by inserting new timing information and may also remap the PIDs if required (and may also modify the PSI information if necessary) to assure that the stream is a proper MPEG transport stream that carries a unique set of PIDs appropriate to the destination subscriber terminal for the current session.

Note that the PIDs may be remapped for storage on the VOD server, but this remapping only segregates the "critical" and "non-critical" content. Prior to transmission to the subscriber, the PIDs can be remapped to assure that each instance of the content playback associated with each VOD session carries a unique set of PIDs that are used by the individual subscriber terminal associated with the particular VOD session. Thus, the same content may be sent to many subscribers using different sets of PIDs in order to distinguish the different sessions.

In accordance with the above example, the legacy encryption device 116 is lightly loaded since it may only have to process roughly 2-10% of the content ultimately destined to the subscriber terminal 50. Accordingly, the headend and network can utilize fewer legacy encryption devices 116 resulting in reduced capital expenditures and reduced hardware requirements.

In this example, if the selectively encrypted content is destined for a subscriber terminal 50 that is enabled for alternate encryption, the session manager 26 provisions the alternate CA system 112 to carry out the encryption processing of the stream. Alternate CA system 112 thus provisions the alternate encryption device to encrypt packets bearing the PIDs of the "critical" packets. In this case, the "critical" packets as well as the "non-critical" packets are routed through routing matrix 120 along path 134 to routing matrix 124 to add/drop re-multiplexer 128 to the alternate encryption device 132. The retimed stream from the add/drop re-multiplexer 128 is then selectively encrypted (or fully encrypted) at the alternate encryption device 132 before being routed via edge resources 46 to the subscriber terminal 50.

It is noted that the edge resources 46 is shown to incorporate QAM and RF functions. However, in many configurations, the edge resources may also incorporate any or all of the alternate encryption device 132, the add/drop re-multiplexer 128 and possibly even the routing matrix 124.

Thus, in accordance with certain embodiments consistent with the present invention, a Video On Demand (VOD) server arrangement has a device for receiving content from a selective encryption processor that processes content to be delivered in a VOD method by selecting first portions of the content for encryption under a selective encryption system and selecting second portions of the content to remain unencrypted. At least one computer readable storage device is incorporated and a processor that: stores the first and second portions in the at least one computer readable storage device; receives a request for delivery of the content, the request being from a terminal having decryption capabilities associated with either a first decryption method or a second decryption method; and determines if the request is from a terminal having decryption capabilities associated with a first decryption method or a second decryption method. If the request is from a terminal having decryption capabilities associated with the first decryption method, then a routing arrangement routes the first portions to a first encryption device and routes the second portions around the first encryption device. A first encryption device encrypts the first portions using a first encryption process to produce encrypted first portions; and the stream of selectively encrypted content is assembled from the encrypted first portions and the second portions.

In a further embodiment, if the request is from a terminal having decryption capabilities associated with the second decryption method: the stream of content is assembled from the first portion and the second portion; the routing mechanism routes the stream to a second encryption device; and a second encryption device encrypts the first portion using a second encryption process to produce a selectively encrypted stream.

In accordance with the above example, the process 200 depicted in **FIGURE 3** can be utilized starting at 204. In this embodiment, the content is stored on the VOD server 22 with "critical" packets identified, e.g., using a new PID. When a request is

received for content from a subscriber terminal 50 at 212, a determination is made as to the decryption capability of the subscriber terminal 50 (e.g., STB) at 216. If the subscriber terminal is enabled for a first encryption system (e.g., a legacy encryption system) at 216, control passes to 222 where "critical" packets are routed to a CA1 enabled encryption device (116) for encryption of the selected packets. "Non-critical" packets are routed around the CA1 enabled encryption device 116 at 226. At 230, the stream is reconstituted and retimed by appropriately interleaving and retiming the encrypted "critical" packets with the "non-critical" packets. The reconstituted selectively encrypted content is then routed to the subscriber terminal 50 at 236 and the process returns at 240.

In the event it is determined that the subscriber terminal is enabled for a second encryption system (CA2) at 216, control passes to 244 where both the "critical" and the "non-critical" packets are routed around the CA1 encryption device. The packets are retimed and interleaved to reconstitute the stream at 248. The reconstituted stream is then passed through the CA2 encryption device at 252 for selective encryption of the "critical" content to produce a selectively encrypted stream. Control then passes to 236 as before.

Thus, according to certain embodiments, a VOD method involves processing content by selecting first portions of the content for encryption under a selective encryption system and selecting second portions of the content to remain unencrypted. The first portions and the second portions are stored. Upon receipt of a request for delivery of the content, the process involves determining if the request is from a terminal having decryption capabilities associated with a first decryption method or a second decryption method. If the request is from a terminal having decryption capabilities associated with the first decryption method, then the process involves routing the first portions to a first encryption device; routing the second portions around the first encryption device; encrypting the first portions using a first encryption process at the first encryption device to produce encrypted first portions; and assembling a stream of selectively encrypted content from the encrypted first portions and the second portions.

In a further embodiment, if the request is from a terminal having decryption capabilities associated with the second decryption method, then the process involves assembling a stream of content from the first portion and the second portion; routing the stream to a second encryption device; and encrypting the first portions using a second encryption process at the second encryption device to produce a selectively encrypted stream.

If the selective encryption processing of the stream during loading of the content onto the VOD server 22 is eliminated, the storage requirement and complexity of the session playback are reduced since the routing decisions around the legacy encryption device(s) can optionally be eliminated. This arrangement also eliminates the need for the add/drop multiplexer and the remapping of PIDs to reconstitute a full transport stream. However, the negative aspect of this version of the topology is additional legacy encryption equipment since the full transport multiplex for each legacy session is passed through the legacy encryption device. Thus many more (perhaps ten to fifty times more) legacy encryption devices are used to provide the same level of service than the system described above.

In certain embodiments, the advantage offered is the savings in hardware and capital equipment required to add a conditional access system to an existing VOD system, which presently has no multiple encryption capability, as is the case at present in most U.S. cable systems. Additionally, it does not create a capital cost penalty to introduce two concurrent yet independent CA systems to a VOD system since some 70% of the systems currently deployed have QAM edge devices containing latent capability to perform CA encryption (such devices are commercially available from Harmonic NSG).

In the composite session-based encryption of VOD content, a new session is initiated in which the VOD session manager determines which conditional access format is compatible with the requesting subscriber terminal equipment (e.g., set top box) based upon information received directly from the subscriber equipment or from another resource such as the billing system 34. The VOD session manager 26 then determines the path to the appropriate encryption resource(s) having access to an RF node serving

the subscriber's service area. The process that follows then depends upon what type of encryption equipment is employed to provide the VOD content to the subscriber.

If the session is destined for a legacy encryption enabled subscriber terminal, the session manager initiates encryption of the session via the legacy CA system 108, which in turn provisions the legacy encryption device 116. The legacy CA system is commanded only to process packets bearing the PIDs representing "critical" content to be encrypted. The remaining content (the bulk of the content) is identified by a different PID and is left unencrypted, and in fact bypasses the legacy encryption device 116. The edge devices which may contain add/drop multiplex, second CA encryption and QAM modulator elements, is configured by the session manager 26 to remap the segregated "critical" content and "non-critical" data back to a single, common PID. If the "critical" content is stored in a separate file on the VOD server 22, then the two files representing the entire content is streamed. In this case, routing matrix 120 is also tasked to send the "non-critical" content around the legacy encryption device via path 134, thus freeing bandwidth from the encrypter so that roughly a 10 to 50 fold improvement in session capacity can be realized on a single encryption device. The bypass stream is recovered as part of the functions of routing matrix 124. The "non-critical" and encrypted "critical" content streams are still recombined into a single stream at the add/drop re-multiplexer 128, which may be incorporated into the edge device.

If the session is destined for a non-legacy encryption enabled subscriber terminal, the session manager 26 initiates the encryption of the session via the alternative conditional access system 112, which in turn provisions the alternate CA encryption device 132. The alternative CA system is commanded to process all the PIDs on the original transport PID, which initially carries only the "non-critical" content. The session manager 26 configures the routing matrix 120 and 124 to send the content along path 134 to bypass the legacy encryption device, which has no function in delivery of content to a non-legacy encryption enabled subscriber terminal. The add/drop re-multiplexer 128, the second CA encrypter 132 and the QAM modulator and RF elements 46 are configured by the session manager 26 to re-map the segregated "critical" data and the "non-critical"

data back to a single, common PID which is then subsequently encrypted as described above at alternate encryption device 132. If the "critical" content is stored in a separate file on the VOD server 22, then the two files representing the entire content selection is streamed to the subscriber terminal. In this case, the "non-critical" and "critical" content streams are still recombined into a single stream (e.g., at add/drop re-multiplexer or other location in the edge devices) prior to alternative encryption.

In a variation of the above embodiments, the "critical" and "non-critical" content can be stored as a single file at VOD server 22. In this example, the full content ("critical" and "non-critical") is routed through either the legacy encryption device 116 or the alternate encryption device 132. Alternatively, the content from the single file can be routed based upon PID by routing matrix 120 either to legacy encryption device 116 or routing matrix 124, essentially splitting the single file for selective encryption before reconstitution of the stream. In this process, blocks 208 and 212 of process 200 are modified to reflect that the content is stored in a single file and that the file is split into "critical" and "non-critical" content upon receipt of a request for the content. Other variations will occur to those skilled in the art upon consideration of the present teachings.

Thus, in certain embodiments consistent with the present invention, a Video On Demand (VOD) method involves receiving a request for delivery of content; retrieving the content from a storage medium; processing the retrieved content by selecting first portions of the content for encryption under a selective encryption system and selecting second portions of the content to remain unencrypted; and determining if the request is from a terminal having decryption capabilities associated with a first decryption method or a second decryption method. If the request is from a terminal having decryption capabilities associated with the first decryption method, then the process involves routing the first portions to a first encryption device; routing the second portions around the first encryption device; encrypting the first portions using a first encryption process at the first encryption device to produce encrypted first portions; and assembling a stream of selectively encrypted content from the encrypted first portions and the second portions.

In a further embodiment, if the request is from a terminal having decryption capabilities associated with the second decryption method, then the embodiment involves assembling a stream of content from the first portion and the second portion; routing the stream to a second encryption device; and encrypting the first portions using a second encryption process at the second encryption device to produce a selectively encrypted stream.

Those skilled in the art will recognize, upon consideration of the above teachings, that certain of the above exemplary embodiments are based upon use of a programmed processor serving, for example, as video server or servers 22 or session manager 26. However, the invention is not limited to such exemplary embodiments, since other embodiments could be implemented using hardware component equivalents such as special purpose hardware and/or dedicated processors. Similarly, general purpose computers, microprocessor based computers, micro-controllers, optical computers, analog computers, dedicated processors, application specific circuits and/or dedicated hard wired logic may be used to construct alternative equivalent embodiments.

Those skilled in the art will appreciate, upon consideration of the above teachings, that the program operations and processes and associated data used to implement certain of the embodiments described above can be implemented using disc storage as well as other forms of storage such as for example Read Only Memory (ROM) devices, Random Access Memory (RAM) devices, network memory devices, optical storage elements, magnetic storage elements, magneto-optical storage elements, flash memory, core memory and/or other equivalent volatile and non-volatile storage technologies without departing from certain embodiments of the present invention. Such alternative storage devices should be considered equivalents.

Certain embodiments described herein, are or may be implemented using a programmed processor executing programming instructions that are broadly described above in flow chart form that can be stored on any suitable electronic or computer readable storage medium and / or can be transmitted over any suitable electronic communication medium. However, those skilled in the art will appreciate, upon

consideration of the present teaching, that the processes described above can be implemented in any number of variations and in many suitable programming languages without departing from embodiments of the present invention. For example, the order of certain operations carried out can often be varied, additional operations can be added or operations can be deleted without departing from certain embodiments of the invention. Error trapping can be added and/or enhanced and variations can be made in user interface and information presentation without departing from certain embodiments of the present invention. Such variations are contemplated and considered equivalent.

While certain embodiments herein were described in conjunction with specific circuitry that carries out the functions described, other embodiments are contemplated in which the circuit functions are carried out using equivalent software or firmware embodiments executed on one or more programmed processors. General purpose computers, microprocessor based computers, micro-controllers, optical computers, analog computers, dedicated processors, application specific circuits and/or dedicated hard wired logic and analog circuitry may be used to construct alternative equivalent embodiments. Other embodiments could be implemented using hardware component equivalents such as special purpose hardware and/or dedicated processors.

Software and/or firmware embodiments may be implemented using a programmed processor executing programming instructions that in certain instances are broadly described above in flow chart form that can be stored on any suitable electronic or computer readable storage medium (such as, for example, disc storage, Read Only Memory (ROM) devices, Random Access Memory (RAM) devices, network memory devices, optical storage elements, magnetic storage elements, magneto-optical storage elements, flash memory, core memory and/or other equivalent volatile and non-volatile storage technologies) and / or can be transmitted over any suitable electronic communication medium. However, those skilled in the art will appreciate, upon consideration of the present teaching, that the processes described above can be implemented in any number of variations and in many suitable programming languages without departing from embodiments of the present invention. For example, the order of

certain operations carried out can often be varied, additional operations can be added or operations can be deleted without departing from certain embodiments of the invention. Error trapping can be added and/or enhanced and variations can be made in user interface and information presentation without departing from certain embodiments of the present invention. Such variations are contemplated and considered equivalent.

While certain illustrative embodiments have been described, it is evident that many alternatives, modifications, permutations and variations will become apparent to those skilled in the art in light of the foregoing description.

What is claimed is: